(80) Der Überwachungsrahmen hängt weitgehend vom Ausmaß der Zusammenarbeit zwischen der federführenden Überwachungsbehörde und dem kritischen IKT-Drittdienstleister ab, der Dienste für Finanzunternehmen bereitstellt, die sich auf die Erbringung von Finanzdienstleistungen auswirken. Eine erfolgreiche Überwachung setzt unter anderem voraus, dass die federführende Überwachungsbehörde in der Lage ist, Überwachungsmissionen und Inspektionen effektiv durchzuführen, um die von kritischen IKT-Drittdienstleistern angewandten Regeln, Kontrollen und Verfahren sowie die potenziellen kumulativen Auswirkungen ihrer Tätigkeiten auf die Finanzstabilität und die Integrität des Finanzsystems zu bewerten. Gleichzeitig ist es entscheidend, dass kritische IKT-Drittdienstleister die Empfehlungen der federführenden Überwachungsbehörde befolgen und deren Bedenken ausräumen. Da ein kritischer IKT-Drittdienstleister, der Dienste bereitstellt, die sich auf die Erbringung von Finanzdienstleistungen auswirken, durch seine mangelnde Zusammenarbeit — beispielsweise indem er den Zugang zu seinen Räumlichkeiten oder die Übermittlung von Informationen verweigert — der federführenden Überwachungsbehörde letztlich ihre wichtigsten Instrumente zur Bewertung des IKT-Drittparteienrisikos nehmen würde und die Finanzstabilität und die Integrität des Finanzsystems dadurch beeinträchtigt werden könnten, ist auch eine angemessene Sanktionsregelung vorzusehen.

(81) Vor diesem Hintergrund sollte die Anforderung, dass eine federführende Überwachungsbehörde Zwangsgelder verhängen können muss, um kritische IKT-Drittdienstleister zur Einhaltung der in dieser Verordnung festgelegten Transparenz- und Zugangsverpflichtungen zu zwingen, nicht durch Schwierigkeiten gefährdet werden, die bei der Durchsetzung dieser Zwangsgelder in Bezug auf kritische IKT-Drittdienstleister mit Sitz in einem Drittland auftreten können. Um solche Sanktionen durchsetzen zu können und eine rasche Aufnahme von Verfahren zur Wahrung der Verteidigungsrechte kritischer IKT-Drittdienstleister im Zusammenhang mit dem Einstufungsmechanismus und der Herausgabe von Empfehlungen zu ermöglichen, sollten diese kritische IKT-Drittdienstleister, die Dienste für Finanzunternehmen bereitstellen, die sich auf die Erbringung von Finanzdienstleistungen auswirken, dazu verpflichtet werden, eine angemessene geschäftliche Präsenz in der Union aufrechtzuerhalten. Aufgrund der Art der Überwachung und fehlender vergleichbarer Regelungen in anderen Rechtsordnungen gibt es keine geeigneten alternativen Mechanismen, die diesem Ziel genügen, indem bei der Überwachung der Auswirkungen digitaler operationeller Risiken, die von systemrelevanten, als kritisch eingestuften IKT-Drittdienstleistern mit Sitz in einem Drittland ausgehen, effektiv mit den Finanzaufsichtsbehörden in Drittländern zusammengearbeitet wird. Um weiterhin kontinuierlich IKT-Dienstleistungen für Finanzunternehmen in der Union bereitstellen zu können, sollte ein IKT-Drittdienstleister mit Sitz in einem Drittland, der als kritisch im Sinne dieser Verordnung eingestuft worden ist, daher innerhalb von zwölf Monaten nach dieser Einstufung alle erforderlichen Vorkehrungen treffen, um seine Eingliederung in die Union mittels Gründung eines Tochterunternehmens im Sinne des Besitzstands der Union, namentlich der Richtlinie 2013/34/EU des Europäischen Parlaments und des Rates ([21]), sicherzustellen.

(82) Die Anforderung, in der Union ein Tochterunternehmen zu gründen, sollte den kritischen IKT-Drittdienstleister nicht daran hindern, IKT-Dienstleistungen und damit verbundene technische Unterstützung von außerhalb der Union gelegenen Einrichtungen und Infrastruktur aus bereitzustellen. Diese Verordnung auferlegt keine Verpflichtung zur Lokalisierung von Daten, da sie keine Speicherung oder Verarbeitung von Daten in der Union vorschreibt.

(83) Kritische IKT-Drittdienstleister sollten in der Lage sein, IKT-Dienstleistungen von jedem beliebigen Ort der Welt aus zu erbringen, nicht unbedingt oder ausschließlich von einem in der Union gelegenen Ort aus. Die Überwachungstätigkeiten sollten zunächst an einem Ort in der Union und im Wege der Interaktion mit in der Union gelegenen Unternehmen, einschließlich der von kritischen IKT-Drittdienstleistern im Sinne dieser Verordnung gegründeten Tochterunternehmen, durchgeführt werden. Diese Maßnahmen innerhalb der Union reichen jedoch möglicherweise nicht aus, um der federführenden Überwachungsbehörde die uneingeschränkte und wirksame Wahrnehmung ihrer Aufgaben im Rahmen dieser Verordnung zu ermöglichen. Die federführende Überwachungsbehörde sollte daher ihre einschlägigen Überwachungsbefugnisse auch in Drittländern ausüben können. Durch die Ausübung dieser Befugnisse in Drittländern sollte es der federführenden Überwachungsbehörde möglich sein, die Einrichtungen zu prüfen, von denen aus die IKT-Dienstleistungen oder die technischen Unterstützungsdienste tatsächlich von dem kritischen IKT-Drittdienstleister bereitgestellt oder betrieben werden, und ein umfassendes und operatives Verständnis des IKT-Risikomanagements des kritischen IKT-Drittdienstleisters zu erhalten. Die Möglichkeit, dass die federführende Überwachungsbehörde als Agentur der Union Befugnisse außerhalb des Gebiets der Union ausübt, sollte durch Festschreibung der einschlägigen Voraussetzungen, insbesondere der Zustimmung des betreffenden kritischen IKT-Drittdienstleisters, klar geregelt werden. Ebenso sollten die einschlägigen Behörden des Drittlandes darüber unterrichtet sein, welche Tätigkeiten die federführende Überwachungsbehörde im Hoheitsgebiet des

([21]) Richtlinie 2013/34/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 über den Jahresabschluss, den konsolidierten Abschluss und damit verbundene Berichte von Unternehmen bestimmter Rechtsformen und zur Änderung der Richtlinie 2006/43/EG des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinien 78/660/EWG und 83/349/EWG des Rates (ABl. L 182 vom 29.6.2013, S. 19).

betreffenden Drittlands ausübt, und keine Einwände dagegen erhoben haben. Um jedoch eine effiziente Umsetzung zu gewährleisten, müssen diese Befugnisse unbeschadet der jeweiligen Zuständigkeiten der Organe der Union bzw. der Mitgliedstaaten beim Abschluss von Vereinbarungen über die Verwaltungszusammenarbeit mit den einschlägigen Behörden des betreffenden Drittlands darin vollständig verankert werden. Diese Verordnung sollte es den ESA daher ermöglichen, mit den einschlägigen Behörden von Drittländern Vereinbarungen über die Verwaltungszusammenarbeit zu schließen, die keine anderweitigen rechtlichen Verpflichtungen gegenüber der Union und ihren Mitgliedstaaten begründen sollten.

(84) Um die Kommunikation mit der federführenden Überwachungsbehörde zu erleichtern und eine angemessene Vertretung sicherzustellen, sollten kritische IKT-Drittdienstleister, die Teil einer Gruppe sind, eine juristische Person als ihre Koordinierungsstelle benennen.

(85) Der Überwachungsrahmen sollte die Befugnis der Mitgliedstaaten unberührt lassen, eigene Aufsichts- oder Überwachungsmissionen in Bezug auf IKT-Drittdienstleister durchzuführen, die im Rahmen dieser Verordnung zwar nicht als kritisch eingestuft werden, aber auf nationaler Ebene als wichtig angesehen werden.

(86) Um die mehrschichtige institutionelle Architektur im Bereich der Finanzdienstleistungen zu nutzen, sollte der Gemeinsame Ausschuss der ESA im Einklang mit seinen Aufgaben im Bereich Cybersicherheit weiterhin die sektorübergreifende Gesamtkoordinierung für alle Fragen im Zusammenhang mit IKT-Risiken gewährleisten. Er sollte dabei durch einen neuen Unterausschuss (Überwachungsforum) unterstützt werden, der sowohl Einzelentscheidungen, die sich an kritische IKT-Drittdienstleister richten, als auch die Herausgabe gemeinsamer Empfehlungen, insbesondere in Bezug auf das Benchmarking der Überwachungsprogramme kritischer IKT-Drittdienstleister und zur Ermittlung bewährter Verfahren zur Bewältigung von Problemen im Zusammenhang mit IKT-Konzentrationsrisiken, vorbereitet.

(87) Um sicherzustellen, dass kritische IKT-Drittdienstleister auf Unionsebene angemessen und wirksam überwacht werden, könnte nach dieser Verordnung jede der drei ESA als federführende Überwachungsbehörde benannt werden. Die Entscheidung darüber, welcher der drei ESA ein kritischer IKT-Drittdienstleister konkret zugewiesen wird, sollte anhand einer Bewertung dessen getroffen werden, welche Finanzunternehmen in den Finanzbranchen, für die die betreffende ESA zuständig ist, überwiegend tätig sind. Dieser Ansatz sollte zu einer ausgewogenen Aufteilung der Aufgaben und Zuständigkeiten zwischen den drei ESA bei der Wahrnehmung ihrer Überwachungsfunktionen führen und die Humanressourcen und das technische Fachwissen, über die jede der drei ESA verfügen, bestmöglich nutzen.

(88) Federführende Überwachungsbehörden sollten mit den erforderlichen Befugnissen ausgestattet werden, Untersuchungen sowie Inspektionen vor Ort und von außerhalb bei kritischen IKT-Drittdienstleistern in deren Räumlichkeiten und an deren Standorten durchzuführen und vollständige und aktuelle Informationen zu erhalten. Diese Befugnisse sollten es der federführenden Überwachungsbehörde ermöglichen, Art, Ausmaß und Auswirkungen des IKT-Drittparteienrisikos für die Finanzunternehmen und letztlich für das Finanzsystem der Union, wahrheitsgetreu erfassen zu können. Die Übertragung der federführenden Überwachung auf die ESA ist eine Voraussetzung dafür, die systemische Dimension des IKT-Risikos im Finanzwesen zu verstehen und zu berücksichtigen. Der Einfluss kritischer IKT-Drittdienstleister auf den Finanzsektor der Union und die potenziellen Probleme, die durch das damit verbundene IKT-Konzentrationsrisiko verursacht werden, erfordern einen kollektiven Ansatz auf Unionsebene. Die gleichzeitige Durchführung mehrfacher Audits und Wahrnehmung von Zugangsrechten, die zahlreiche zuständige Behörden gesondert unter geringer oder keinerlei Abstimmung vornehmen, würden die Finanzaufsichtsbehörden daran hindern, sich einen vollständigen und umfassenden Überblick über das IKT-Drittparteienrisiko in der Union zu verschaffen und zudem gleichzeitig Redundanz, Belastungen und Komplexität für kritische IKT-Drittdienstleister mit sich bringen, wenn sie mit einer Vielzahl von Überwachungs- und Inspektionsanfragen konfrontiert sind.

(89) Aufgrund der erheblichen Auswirkungen, die mit der Einstufung als kritischer IKT-Drittdienstleister verbunden sind, sollte mit dieser Verordnung sichergestellt werden, dass die Rechte kritischer IKT-Drittdienstleister während der Umsetzung des Überwachungsrahmens gewahrt werden. Bevor sie als kritisch eingestuft werden, sollten diese Dienstleister beispielsweise berechtigt sein, der federführenden Überwachungsbehörde eine mit Gründen versehene Erklärung vorzulegen, die alle für die Beurteilung ihrer Einstufung relevanten Informationen enthält. Da die federführende Überwachungsbehörde befugt sein sollte, Empfehlungen zu IKT-Risiken und diesbezüglich geeigneten Abhilfemaßnahmen herauszugeben, was auch die Befugnis einschließt, bestimmte vertragliche Vereinbarungen, die letztlich die Stabilität des Finanzunternehmens oder des Finanzsystems beeinträchtigen, abzulehnen, sollte kritischen IKT-Drittdienstleistern ebenfalls die Möglichkeit eingeräumt werden, vor der Fertigstellung dieser Empfehlungen darzulegen, wie sich die darin aufgezeigten Lösungen voraussichtlich auf

Kunden auswirken werden, bei denen es sich um nicht in den Geltungsbereich dieser Verordnung fallende Unternehmen handelt, sowie Lösungen zur Risikominderung aufzuzeigen. Kritische IKT-Drittdienstleister, die den Empfehlungen nicht zustimmen, sollten eine begründete Erklärung über ihre Absicht, die Empfehlung nicht zu billigen, abgeben. Wird eine solche begründete Erklärung nicht abgegeben oder als unzureichend erachtet, sollte die federführende Überwachungsbehörde eine Mitteilung veröffentlichen, in der die strittige Angelegenheit kurz dargelegt wird.

(90) Die zuständigen Behörden sollten die Aufgabe, die inhaltliche Einhaltung der von der federführenden Überwachungsbehörde herausgegebenen Empfehlungen zu überprüfen, im Rahmen ihrer Tätigkeiten zur Beaufsichtigung von Finanzunternehmen gebührend wahrnehmen. Die zuständigen Behörden sollten Finanzunternehmen dazu verpflichten können, zusätzliche Maßnahmen zu ergreifen, um den in den Empfehlungen der federführenden Überwachungsbehörde ermittelten Risiken zu begegnen, und sollten zu gegebener Zeit entsprechende Mitteilungen herausgeben. Richtet die federführende Überwachungsbehörde Empfehlungen an kritische IKT-Drittdienstleister, die gemäß der Richtlinie (EU) 2022/2555 beaufsichtigt werden, so sollten die zuständigen Behörden auf freiwilliger Basis und vor dem Erlass zusätzlicher Maßnahmen die gemäß der genannten Richtlinie zuständigen Behörden konsultieren können, um einen koordinierten Ansatz in Bezug auf die betreffenden kritischen IKT-Drittdienstleister zu erleichtern.

(91) Die Ausübung der Überwachung sollte sich an drei Handlungsgrundsätzen orientieren, um Folgendes sicherzustellen: a) eine enge Koordinierung zwischen den ESA bei ihren Aufgaben als federführende Überwachungsbehörde mithilfe eines gemeinsamen Überwachungsnetzes (JON — Joint Oversight Network), b) die Kohärenz mit dem durch die Richtlinie (EU) 2022/2555 geschaffenen Rahmen (über eine freiwillige Konsultation der Einrichtungen, die in den Geltungsbereich der genannten Richtlinie fallen, um Doppelarbeit bei an kritische IKT-Drittdienstleister gerichteten Maßnahmen zu vermeiden) und c) eine Sorgfaltspflicht, wonach das potenzielle Risiko einer Störung der von kritischen IKT-Drittdienstleistern bereitgestellten Dienste für Kunden, bei denen es sich um nicht in den Geltungsbereich dieser Verordnung fallende Unternehmen handelt, zu minimieren ist.

(92) Der Überwachungsrahmen sollte nicht die Anforderung an Finanzunternehmen ersetzen, die Risiken, die die Nutzung von IKT-Drittdienstleistern mit sich bringt, selbst zu managen und sollte weder in irgendeiner Form noch für irgendeinen Aspekt an deren Stelle treten; dies schließt auch die Verpflichtung ein, die laufende Überwachung der mit kritischen IKT-Drittdienstleistern geschlossenen vertraglichen Vereinbarungen aufrechtzuerhalten. Ebenso sollte der Überwachungsrahmen die volle Verantwortung der Finanzunternehmen für die Einhaltung und Erfüllung aller Verpflichtungen gemäß dieser Verordnung und dem einschlägigen Finanzdienstleistungsrecht unberührt lassen.

(93) Um Doppelarbeit und Überschneidungen zu vermeiden, sollten die zuständigen Behörden davon absehen, im Alleingang Maßnahmen zur Überwachung des von kritischen IKT-Drittdienstleistern ausgehenden Risikos zu ergreifen, und sollten sich diesbezüglich auf die einschlägige Bewertung der federführenden Überwachungsbehörde stützen. Sämtliche Maßnahmen sollten in jedem Fall zuvor mit der federführenden Überwachungsbehörde im Rahmen der Ausübung ihrer Aufgaben innerhalb des Überwachungsrahmens koordiniert und vereinbart werden.

(94) Um auf internationaler Ebene die Konvergenz in Bezug auf bewährte Verfahren zu fördern, die für die Überprüfung und Überwachung des Managements von IKT-Drittdienstleistern ausgehender digitaler Risiken zu nutzen sind, sollten die ESA aufgefordert werden, Kooperationsvereinbarungen mit den zuständigen Aufsichts- und Regulierungsbehörden in Drittländern zu schließen.

(95) Um die speziellen Qualifikationen, die technischen Kompetenzen und das Fachwissen des auf operationelle und IKT-Risiken spezialisierten Personals innerhalb der zuständigen Behörden, der drei ESA und — auf freiwilliger Basis — der gemäß der Richtlinie (EU) 2022/2555 zuständigen Behörden zu nutzen, sollte die federführende Überwachungsbehörde auf nationale Aufsichtsfähigkeiten und das entsprechende Fachwissen zurückgreifen und für jeden einzelnen kritischen IKT-Drittdienstleister spezielle Untersuchungsteams einrichten und multidisziplinäre Teams zusammenlegen, um sowohl die Vorbereitung als auch die tatsächliche Wahrnehmung von Überwachungstätigkeiten zu unterstützen, einschließlich allgemeiner Untersuchungen und Inspektionen kritischer IKT-Drittdienstleister sowie jeglicher erforderlichen Folgemaßnahmen.

(96) Während die Kosten, die sich aus den Überwachungsaufgaben ergeben, vollständig aus Gebühren finanziert würden, die von kritischen IKT-Drittdienstleistern erhoben werden, dürften den ESA hingegen vor Beginn des Überwachungsrahmens Kosten für die Einführung spezieller IKT-Systeme zur Unterstützung der anstehenden Überwachung entstehen, da im Vorfeld spezielle IKT-Systeme entwickelt und eingeführt werden müssten. Diese Verordnung sieht daher ein hybrides Finanzierungsmodell vor, bei dem der Überwachungsrahmen als solcher vollständig gebührenfinanziert wäre, während die Entwicklung der IKT-Systeme der ESA aus Beiträgen der Union und der zuständigen nationalen Behörden finanziert würde.

(97) Zuständige Behörden sollten über alle erforderlichen Aufsichts-, Untersuchungs- und Sanktionsbefugnisse verfügen, um die angemessene Wahrnehmung ihrer Aufgaben im Rahmen dieser Verordnung sicherzustellen. Sie sollten grundsätzlich die von ihnen verhängten Verwaltungssanktionen öffentlich bekannt machen. Da Finanzunternehmen und kritische IKT-Drittdienstleister in unterschiedlichen Mitgliedstaaten ansässig sein und der Aufsicht unterschiedlicher zuständiger Behörden unterliegen können, sollte die Anwendung dieser Verordnung zum einen durch die enge Zusammenarbeit zwischen den jeweils zuständigen Behörden, einschließlich der EZB bei der Wahrnehmung der ihr durch die Verordnung (EU) Nr. 1024/2013 übertragenen besonderen Aufgaben, erleichtert werden sowie zum anderen durch die Abstimmung mit den ESA im Wege des gegenseitigen Informationsaustauschs und der Erbringung von Amtshilfe in den einschlägigen Aufsichtsbelangen.

(98) Um die Kriterien für die Einstufung von IKT-Drittdienstleistern als kritisch weiter zu quantifizieren und zu präzisieren und um Überwachungsgebühren zu harmonisieren, sollte der Kommission die Befugnis übertragen werden, gemäß Artikel 290 AEUV Rechtsakte zur Ergänzung dieser Verordnung in Bezug auf Folgendes zu erlassen: die weitere Präzisierung der systemischen Auswirkungen, die ein Ausfall eines Dienstes oder ein operativer Ausfall eines IKT-Drittdienstleisters auf die Finanzunternehmen haben könnte, für die er IKT-Dienstleistungen bereitstellt; die Anzahl global systemrelevanter Institute (G-SRI) oder anderer systemrelevanter Institute (A-SRI), die auf den betreffenden IKT-Drittdienstleister angewiesen sind; die Zahl der IKT-Drittdienstleister, die auf einem bestimmten Markt tätig sind; die Kosten für die Migration von Daten und IKT-Arbeitslasten zu anderen IKT-Drittdienstleistern; sowie den Betrag der Überwachungsgebühren und die damit verbundene Zahlungsweise. Es ist von besonderer Bedeutung, dass die Kommission im Zuge ihrer Vorbereitungsarbeit angemessene Konsultationen, auch auf der Ebene von Sachverständigen, durchführt, die mit den Grundsätzen in Einklang stehen, die in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung ([22]) niedergelegt wurden. Um insbesondere für eine gleichberechtigte Beteiligung an der Vorbereitung delegierter Rechtsakte zu sorgen, sollten das Europäische Parlament und der Rat alle Dokumente zur gleichen Zeit wie die Sachverständigen der Mitgliedstaaten erhalten, und ihre Sachverständigen sollten systematisch Zugang zu den Sitzungen der Sachverständigengruppen der Kommission haben, die mit der Vorbereitung der delegierten Rechtsakte befasst sind.

(99) Die kohärente Harmonisierung der in dieser Verordnung festgelegten Anforderungen sollte durch technische Regulierungsstandards gewährleistet werden. In ihrer Funktion als Stellen, die über hochspezialisierte Fachkräfte verfügen, sollten die ESA Entwürfe technischer Regulierungsstandards ausarbeiten, die keine politischen Entscheidungen erfordern, und sie der Kommission vorlegen. In den Bereichen IKT-Risikomanagement, Meldung schwerwiegender IKT-bezogener Vorfälle, Tests sowie in Bezug auf Schlüsselanforderungen für eine solide Überwachung des IKT-Drittparteienrisikos sollten technische Regulierungsstandards entwickelt werden. Die Kommission und die ESA sollten sicherstellen, dass diese Standards und Anforderungen von allen Finanzunternehmen auf eine Weise angewandt werden können, die ihrer Größe und ihrem Gesamtrisikoprofil sowie der Art, dem Umfang und der Komplexität ihrer Dienstleistungen, Tätigkeiten und Geschäfte angemessen ist. Der Kommission sollte die Befugnis übertragen werden, diese technischen Regulierungsstandards mittels delegierter Rechtsakten gemäß Artikel 290 AEUV und im Einklang mit den Artikeln 10 und 14 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 zu erlassen.

(100) Um die Vergleichbarkeit der Meldungen über schwerwiegende IKT-bezogene Vorfälle und schwerwiegende zahlungsbezogene Betriebs- oder Sicherheitsvorfälle zu erleichtern sowie um für Transparenz in Bezug auf vertragliche Vereinbarungen über die Nutzung von IKT-Dienstleistungen von Drittdienstleistern zu sorgen, sollten die ESA Entwürfe technischer Durchführungsstandards erarbeiten, mit denen standardisierte Vorlagen, Formulare und Verfahren für Finanzunternehmen zur Meldung schwerwiegender IKT-bezogener Vorfälle und schwerwiegender zahlungsbezogener Betriebs- oder Sicherheitsvorfälle sowie standardisierte Vorlagen für das Informationsregister festgelegt werden. Bei der Ausarbeitung dieser Standards sollten die ESA die Größe und das Gesamtrisikoprofil des Finanzunternehmens sowie die Art, den Umfang und die Komplexität seiner Dienstleistungen, Tätigkeiten und Geschäfte berücksichtigen. Der Kommission sollte die Befugnis übertragen werden, diese technischen Durchführungsstandards mittels Durchführungsrechtsakten gemäß Artikel 291 AEUV und im Einklang mit Artikel 15 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 zu erlassen.

([22]) ABl. L 123 vom 12.5.2016, S. 1.

(101) Da weitere Anforderungen bereits durch delegierte Rechtsakte und Durchführungsrechtsakte auf der Grundlage technischer Regulierungs- und Durchführungsstandards in den Verordnungen (EG) Nr. 1060/2009 ([23]), (EU) Nr. 648/2012 ([24]), (EU) Nr. 600/2014 ([25]) bzw. (EU) Nr. 909/2014 ([26]) des Europäischen Parlaments und des Rates festgelegt wurden, ist es angezeigt, die ESA entweder einzeln oder gemeinsam über den Gemeinsamen Ausschuss zu beauftragen, der Kommission technische Regulierungs- und Durchführungsstandards für den Erlass von delegierten Rechtsakten und Durchführungsrechtsakten zur Übernahme und Aktualisierung bestehender IKT-Risikomanagementvorschriften vorzulegen.

(102) Da die vorliegende Verordnung in Verbindung mit der Richtlinie (EU) 2022/2556 des Europäischen Parlaments und des Rates ([27]) eine Konsolidierung der Bestimmungen über IKT-Risikomanagement mit sich bringt, die sich über mehrere Verordnungen und Richtlinien des Besitzstands der Union im Bereich der Finanzdienstleistungen erstrecken, einschließlich der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014 und (EU) Nr. 909/2014 und der Verordnung (EU) 2016/1011 ([28]) des Europäischen Parlaments und des Rates, sollten diese Verordnungen zur Gewährleistung vollständiger Übereinstimmung geändert werden, damit klargestellt ist, dass die geltenden Bestimmungen über IKT-Risiken in der vorliegenden Verordnung verankert sind.

(103) Der Geltungsbereich der einschlägigen Artikel über operationelle Risiken, auf deren Grundlage durch Befugnisübertragungen gemäß den Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014 (EU) Nr. 909/2014 und (EU) 2016/1011 der Erlass von delegierten Rechtsakten und Durchführungsrechtsakten ermöglicht wurde, sollte folglich eingeschränkt werden, damit alle Bestimmungen, die Aspekte der digitalen operationalen Resilienz betreffen und heute Teil der genannten Verordnungen sind, in die vorliegende Verordnung übernommen werden können.

(104) Das potenzielle systemische Cyberrisiko, das mit der Nutzung von IKT-Infrastrukturen verbunden ist, die den Betrieb von Zahlungssystemen und die Erbringung von Zahlungsabwicklungstätigkeiten ermöglichen, sollte auf Unionsebene durch harmonisierte Vorschriften für die digitale Resilienz angemessen angegangen werden. Zu diesem Zweck sollte die Kommission rasch prüfen, ob der Geltungsbereich der vorliegenden Verordnung überprüft werden muss, und diese Überprüfung zugleich an die Ergebnisse der in der Richtlinie (EU) 2015/2366 vorgesehenen umfassenden Überprüfung anpassen. Zahlreiche Großangriffe in den letzten zehn Jahren haben gezeigt, inwiefern Zahlungssysteme Cyberbedrohungen ausgesetzt sind. Da sie im Mittelpunkt der Zahlungsdienstleistungskette stehen und starke Verflechtungen mit dem gesamten Finanzsystem aufweisen, sind Zahlungssysteme und Zahlungsabwicklungstätigkeiten nunmehr zu einem maßgeblichen Faktor für das Funktionieren der Finanzmärkte der Union geworden. Cyberangriffe auf diese Systeme können zu schwerwiegenden Betriebsstörungen führen, die sich direkt auf wirtschaftliche Schlüsselfunktionen wie die Erleichterung von Zahlungen auswirken und zugleich indirekt Konsequenzen für die damit verbundenen wirtschaftlichen Prozesse haben. Bis zur Einführung eines harmonisierten Systems und der Beaufsichtigung der Betreiber von Zahlungssystemen und Zahlungsabwicklungsunternehmen auf Unionsebene können sich die Mitgliedstaaten zur Anwendung ähnlicher Marktpraktiken an den mit dieser Verordnung festgelegten Anforderungen an die digitale operationale Resilienz orientieren, wenn sie für Betreiber von Zahlungssystemen und Zahlungsabwicklungsunternehmen, die in ihrem jeweiligen Hoheitsgebiet der Aufsicht unterliegen, diesbezügliche Vorschriften anwenden.

([23]) Verordnung (EG) Nr. 1060/2009 des Europäischen Parlaments und des Rates vom 16. September 2009 über Ratingagenturen (ABl. L 302 vom 17.11.2009, S. 1).

([24]) Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates vom 4. Juli 2012 über OTC-Derivate, zentrale Gegenparteien und Transaktionsregister (ABl. L 201 vom 27.7.2012, S. 1).

([25]) Verordnung (EU) Nr. 600/2014 des Europäischen Parlaments und des Rates vom 15. Mai 2014 über Märkte für Finanzinstrumente und zur Änderung der Verordnung (EU) Nr. 648/2012 (ABl. L 173 vom 12.6.2014, S. 84).

([26]) Verordnung (EU) Nr. 909/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 zur Verbesserung der Wertpapierlieferungen und -abrechnungen in der Europäischen Union und über Zentralverwahrer sowie zur Änderung der Richtlinien 98/26/EG und 2014/65/EU und der Verordnung (EU) Nr. 236/2012 (ABl. L 257 vom 28.8.2014, S. 1).

([27]) Richtlinie (EU) 2022/2556 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 zur Änderung der Richtlinien 2009/65/EG, 2009/138/EG, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 und (EU) 2016/2341 hinsichtlich der digitalen operationalen Resilienz im Finanzsektor (siehe Seite 153 dieses Amtsblatts).

([28]) Verordnung (EU) 2016/1011 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über Indizes, die bei Finanzinstrumenten und Finanzkontrakten als Referenzwert oder zur Messung der Wertentwicklung eines Investmentfonds verwendet werden, und zur Änderung der Richtlinien 2008/48/EG und 2014/17/EU sowie der Verordnung (EU) Nr. 596/2014 (ABl. L 171 vom 29.6.2016, S. 1).

(105) Da das Ziel dieser Verordnung, nämlich die Erreichung eines hohen Niveaus an digitaler operationaler Resilienz in beaufsichtigten Finanzunternehmen, von den Mitgliedstaaten nicht ausreichend verwirklicht werden kann, weil es der Harmonisierung einiger unterschiedlicher Vorschriften im Unionsrecht und im nationalen Recht bedarf, sondern vielmehr wegen seines Umfangs und seiner Wirkungen auf Unionsebene besser zu verwirklichen ist, kann die Union im Einklang mit dem in Artikel 5 des Vertrags über die Europäische Union verankerten Subsidiaritätsprinzip tätig werden. Entsprechend dem in demselben Artikel genannten Grundsatz der Verhältnismäßigkeit geht diese Verordnung nicht über das für die Verwirklichung dieses Ziels erforderliche Maß hinaus.

(106) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates ([29]) konsultiert und hat am 10. Mai 2021 eine Stellungnahme abgegeben ([30]) —

HABEN FOLGENDE VERORDNUNG ERLASSEN:

KAPITEL I

Allgemeine Bestimmungen

Artikel 1

Gegenstand

(1) Um ein hohes gemeinsames Niveau an digitaler operationaler Resilienz zu erreichen, werden in dieser Verordnung einheitliche Anforderungen für die Sicherheit von Netzwerk- und Informationssystemen, die die Geschäftsprozesse von Finanzunternehmen unterstützen, wie folgt festgelegt:

a) auf Finanzunternehmen anwendbare Anforderungen in Bezug auf:

   i) Risikomanagement im Bereich der Informations- und Kommunikationstechnologie (IKT);

   ii) Meldung schwerwiegender IKT-bezogener Vorfälle und — auf freiwilliger Basis — erheblicher Cyberbedrohungen an die zuständigen Behörden;

   iii) Meldung schwerwiegender zahlungsbezogener Betriebs- oder Sicherheitsvorfälle durch in Artikel 2 Absatz 1 Buchstaben a bis d aufgeführte Finanzunternehmen an die zuständigen Behörden;

   iv) Tests der digitalen operationalen Resilienz;

   v) Austausch von Informationen und Erkenntnissen in Bezug auf Cyberbedrohungen und Schwachstellen;

   vi) Maßnahmen für das solide Management des IKT-Drittparteienrisikos;

b) Anforderungen in Bezug auf vertragliche Vereinbarungen zwischen IKT-Drittdienstleistern und Finanzunternehmen;

c) Vorschriften über die Einrichtung und Ausführung des Überwachungsrahmens für kritische IKT-Drittdienstleister bei der Erbringung von Dienstleistungen für Finanzunternehmen;

d) Vorschriften über die Zusammenarbeit zwischen zuständigen Behörden und Vorschriften über die Beaufsichtigung und Durchsetzung aller von dieser Verordnung erfassten Sachverhalte durch zuständige Behörden.

(2) In Bezug auf Finanzunternehmen, die gemäß den nationalen Vorschriften zur Umsetzung von Artikel 3 der Richtlinie (EU) 2022/2555 als wesentliche oder wichtige Unternehmen ermittelt wurden, gilt diese Verordnung für die Zwecke von Artikel 4 der genannten Richtlinie als sektorspezifischer Rechtsakt der Union.

(3) Diese Verordnung lässt die Zuständigkeiten der Mitgliedstaaten für grundlegende Funktionen des Staates in Bezug auf die öffentliche Sicherheit, die Landesverteidigung und die nationale Sicherheit im Einklang mit dem Unionsrecht unberührt.

([29]) Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39).

([30]) ABl. C 229 vom 15.6.2021, S. 16.

Artikel 2

Geltungsbereich

(1) Unbeschadet der Absätze 3 und 4 gilt diese Verordnung für folgende Unternehmen:

a) Kreditinstitute,

b) Zahlungsinstitute, einschließlich gemäß der Richtlinie (EU) 2015/2366 ausgenommene Zahlungsinstitute,

c) Kontoinformationsdienstleister,

d) E-Geld-Institute, einschließlich gemäß der Richtlinie 2009/110/EG ausgenommene E-Geld-Institute,

e) Wertpapierfirmen,

f) Anbieter von Krypto-Dienstleistungen, die gemäß einer Verordnung des Europäischen Parlaments und des Rates über Märkte von Krypto-Werten und zur Änderung der Verordnungen (EU) Nr. 1093/2010 und (EU) Nr. 1095/2010 sowie der Richtlinien 2013/36/EU und (EU) 2019/1937 (im Folgenden „Verordnung über Märkte von Krypto-Werten“) zugelassen sind, und Emittenten wertreferenzierter Token,

g) Zentralverwahrer,

h) zentrale Gegenparteien,

i) Handelsplätze,

j) Transaktionsregister,

k) Verwalter alternativer Investmentfonds,

l) Verwaltungsgesellschaften,

m) Datenbereitstellungsdienste,

n) Versicherungs- und Rückversicherungsunternehmen,

o) Versicherungsvermittler, Rückversicherungsvermittler und Versicherungsvermittler in Nebentätigkeit,

p) Einrichtungen der betrieblichen Altersversorgung,

q) Ratingagenturen,

r) Administratoren kritischer Referenzwerte,

s) Schwarmfinanzierungsdienstleister,

t) Verbriefungsregister,

u) IKT-Drittdienstleister.

(2) Für die Zwecke dieser Verordnung werden die in Absatz 1 Buchstaben a bis t genannten Unternehmen zusammen als „Finanzunternehmen“ bezeichnet.

(3) Diese Verordnung gilt nicht für:

a) Verwalter alternativer Investmentfonds im Sinne von Artikel 3 Absatz 2 der Richtlinie 2011/61/EU;

b) Versicherungs- und Rückversicherungsunternehmen im Sinne von Artikel 4 der Richtlinie 2009/138/EG;

c) Einrichtungen der betrieblichen Altersversorgung, die Altersversorgungssysteme mit insgesamt weniger als 15 Versorgungsanwärtern betreiben;

d) gemäß den Artikeln 2 und 3 der Richtlinie 2014/65/EU ausgenommene natürliche oder juristische Personen;

e) Versicherungsvermittler, Rückversicherungsvermittler und Versicherungsvermittler in Nebentätigkeit, bei denen es sich um Kleinstunternehmen oder kleine oder mittlere Unternehmen handelt;

f) Postgiroämter im Sinne von Artikel 2 Absatz 5 Nummer 3 der Richtlinie 2013/36/EU.

(4) Die Mitgliedstaaten können die in Artikel 2 Absatz 5 Nummern 4 bis 23 der Richtlinie 2013/36/EU aufgeführten Stellen, die sich in ihrem jeweiligen Hoheitsgebiet befinden, vom Geltungsbereich dieser Verordnung ausnehmen. Macht ein Mitgliedstaat von dieser Möglichkeit Gebrauch, so setzt er die Kommission hiervon sowie von allen nachfolgenden Änderungen in Kenntnis. Die Kommission macht diese Informationen auf ihrer Website oder auf andere leicht zugängliche Weise öffentlich zugänglich.

Artikel 3

Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck:

1. „digitale operationale Resilienz“ die Fähigkeit eines Finanzunternehmens, seine operative Integrität und Betriebszuverlässigkeit aufzubauen, zu gewährleisten und zu überprüfen, indem es entweder direkt oder indirekt durch Nutzung der von IKT-Drittdienstleistern bereitgestellten Dienste das gesamte Spektrum an IKT-bezogenen Fähigkeiten sicherstellt, die erforderlich sind, um die Sicherheit der Netzwerk- und Informationssysteme zu gewährleisten, die von einem Finanzunternehmen genutzt werden und die kontinuierliche Erbringung von Finanzdienstleistungen und deren Qualität, einschließlich bei Störungen, unterstützen;

2. „Netzwerk- und Informationssystem“ ein Netz- und Informationssystem im Sinne von Artikel 6 Nummer 1 der Richtlinie (EU) 2022/2555;

3. „IKT-Altsystem“ ein IKT-System, das das Ende seines Lebenszyklus (Ende seiner Lebensdauer) erreicht hat, aus technologischen oder wirtschaftlichen Gründen nicht für Upgrades oder Fehlerbehebungen in Frage kommt oder nicht mehr von seinem Anbieter oder einem IKT-Drittdienstleister unterstützt wird, das allerdings weiterhin genutzt wird und die Funktionen des Finanzunternehmens unterstützt;

4. „Sicherheit von Netzwerk- und Informationssystemen“ die Sicherheit von Netz- und Informationssystemen im Sinne von Artikel 6 Nummer 2 der Richtlinie (EU) 2022/2555;

5. „IKT-Risiko“ jeden vernünftigerweise identifizierbaren Umstand im Zusammenhang mit der Nutzung von Netzwerk- und Informationssystemen, der bei Eintritt durch die damit einhergehenden nachteiligen Auswirkungen im digitalen oder physischen Umfeld die Sicherheit der Netzwerk- und Informationssysteme, jeglicher technologieabhängiger Instrumente oder Prozesse, von Geschäften und Prozessen oder der Bereitstellung von Diensten beeinträchtigen kann.

6. „Informationsasset“ eine Sammlung materieller oder immaterieller Informationen, die geschützt werden sollten;

7. „IKT-Asset“ eine Software oder Hardware in den Netzwerk- und Informationssystemen, die das Finanzunternehmen nutzt;

8. „IKT-bezogener Vorfall“ ein von dem Finanzunternehmen nicht geplantes Ereignis bzw. eine entsprechende Reihe verbundener Ereignisse, das bzw. die die Sicherheit der Netzwerk- und Informationssysteme beeinträchtigt und nachteilige Auswirkungen auf die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten oder auf die vom Finanzunternehmen erbrachten Dienstleistungen hat;

9. „zahlungsbezogener Betriebs- oder Sicherheitsvorfall“ ein von den in Artikel 2 Absatz 1 Buchstaben a bis d aufgeführten Finanzunternehmen nicht geplantes Ereignis bzw. eine entsprechende Reihe verbundener Ereignisse, unabhängig davon, ob es sich um IKT-bezogene Vorfälle handelt oder nicht, das bzw. die nachteilige Auswirkungen auf die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit zahlungsbezogener Daten oder auf die vom Finanzunternehmen bereitgestellten zahlungsbezogenen Dienste hat;

10. „schwerwiegender IKT-bezogener Vorfall“ einen IKT-Vorfall, der umfassende nachteilige Auswirkungen auf die Netzwerk- und Informationssysteme hat, die kritische oder wichtige Funktionen des Finanzunternehmens unterstützen;

11. „schwerwiegender zahlungsbezogener Betriebs- oder Sicherheitsvorfall“ einen zahlungsbezogenen Betriebs- oder Sicherheitsvorfall, der umfassende nachteilige Auswirkungen auf die bereitgestellten zahlungsbezogenen Dienste hat;

12. „Cyberbedrohung“ eine Cyberbedrohung im Sinne von Artikel 2 Nummer 8 der Verordnung (EU) 2019/881;

13. „erhebliche Cyberbedrohung“ eine Cyberbedrohung, deren technische Merkmale darauf hindeuten, dass sie das Potenzial haben könnte, einen schwerwiegenden IKT-bezogenen Vorfall oder einen schwerwiegenden zahlungsbezogenen Betriebs- oder Sicherheitsvorfall zu verursachen;

14. „Cyberangriff“ einen böswilligen IKT-bezogenen Vorfall, der auf den Versuch eines Angreifers zurückgeht, einen Vermögenswert zu zerstören, freizulegen, zu verändern, zu deaktivieren, zu entwenden oder auf unberechtigte Weise auf diesen Vermögenswert zuzugreifen oder ihn auf unberechtigte Weise zu nutzen;

15. „Bedrohungsanalyse“ Informationen, die aggregiert, umgewandelt, analysiert, ausgewertet oder erweitert wurden, um den notwendigen Kontext für die Entscheidungsfindung zu schaffen und ein relevantes und ausreichendes Verständnis für die Abmilderung der Auswirkungen eines IKT-bezogenen Vorfalls oder einer Cyberbedrohung zu ermöglichen, einschließlich der technischen Einzelheiten eines Cyberangriffs, der für den Angriff verantwortlichen Personen und ihres Modus Operandi und ihrer Beweggründe;

16. „Schwachstelle“ eine Schwachstelle, Empfindlichkeit oder Fehlfunktion eines Vermögenswerts, eines Systems, eines Prozesses oder einer Kontrolle, die ausgenutzt werden kann;

17. „bedrohungsorientierte Penetrationstests (TLPT — Threat-Led Penetration Testing)“ einen Rahmen, der Taktik, Techniken und Verfahren realer Angreifer, die als echte Cyberbedrohung empfunden werden, nachbildet und einen kontrollierten, maßgeschneiderten, erkenntnisgestützten (Red-Team-) Test der kritischen Live-Produktionssysteme des Finanzunternehmens ermöglicht;

18. „IKT-Drittparteienrisiko“ ein IKT-bezogenes Risiko, das für ein Finanzunternehmen im Zusammenhang mit dessen Nutzung von IKT-Dienstleistungen entstehen kann, die von IKT-Drittdienstleistern oder deren Unterauftragnehmern, einschließlich über Vereinbarungen zur Auslagerung, bereitgestellt werden;

19. „IKT-Drittdienstleister“ ein Unternehmen, das IKT-Dienstleistungen bereitstellt;

20. „gruppeninterner IKT-Dienstleister“ ein Unternehmen, das Teil einer Finanzgruppe ist und überwiegend IKT-Dienstleistungen für Finanzunternehmen derselben Gruppe oder für Finanzunternehmen, die demselben institutsbezogenen Sicherungssystem angehören, bereitstellt, einschließlich deren Mutterunternehmen, Tochterunternehmen und Zweigniederlassungen oder anderer Unternehmen, die in gemeinsamem Eigentum oder unter gemeinsamer Kontrolle stehen;

21. „IKT-Dienstleistungen“ digitale Dienste und Datendienste, die über IKT-Systeme einem oder mehreren internen oder externen Nutzern dauerhaft bereitgestellt werden, einschließlich Hardware als Dienstleistung und Hardwaredienstleistungen, wozu auch technische Unterstützung durch den Hardwareanbieter mittels Software- oder Firmware-Aktualisierungen gehört, mit Ausnahme herkömmlicher analoger Telefondienste;

22. „kritische oder wichtige Funktion“ eine Funktion, deren Ausfall die finanzielle Leistungsfähigkeit eines Finanzunternehmens oder die Solidität oder Fortführung seiner Geschäftstätigkeiten und Dienstleistungen erheblich beeinträchtigen würde oder deren unterbrochene, fehlerhafte oder unterbliebene Leistung die fortdauernde Einhaltung der Zulassungsbedingungen und -verpflichtungen eines Finanzunternehmens oder seiner sonstigen Verpflichtungen nach dem anwendbaren Finanzdienstleistungsrecht erheblich beeinträchtigen würde;

23. „kritischer IKT-Drittdienstleister“ einen IKT-Drittdienstleister, der gemäß Artikel 31 als kritisch eingestuft wurde;

24. „IKT-Drittdienstleister mit Sitz in einem Drittland“ einen IKT-Drittdienstleister, bei dem es sich um eine in einem Drittland niedergelassene juristische Person handelt, die mit einem Finanzunternehmen eine vertragliche Vereinbarung über die Bereitstellung von IKT-Dienstleistungen geschlossen hat;

25. „Tochterunternehmen“ ein Tochterunternehmen im Sinne von Artikel 2 Nummer 10 und Artikel 22 der Richtlinie 2013/34/EU;

26. „Gruppe“ eine Gruppe im Sinne von Artikel 2 Nummer 11 der Richtlinie 2013/34/EU;

27. „Mutterunternehmen“ ein Mutterunternehmen im Sinne von Artikel 2 Nummer 9 und Artikel 22 der Richtlinie 2013/34/EU;

28. „IKT-Unterauftragnehmer mit Sitz in einem Drittland“ einen IKT-Unterauftragnehmer, bei dem es sich um eine in einem Drittland niedergelassene juristische Person handelt, die mit einem IKT-Drittdienstleister oder einem IKT-Drittdienstleister mit Sitz in einem Drittland eine vertragliche Vereinbarung geschlossen hat;

29. „IKT-Konzentrationsrisiko“ die Exposition gegenüber einzelnen oder mehreren verbundenen kritischen IKT-Drittdienstleistern, die zu einer gewissen Abhängigkeit von diesen Dienstleistern führt, sodass die Nichtverfügbarkeit, der Ausfall oder sonstige Defizite dieser Dienstleister die Fähigkeit eines Finanzunternehmens gefährden könnten, kritische oder wichtige Funktionen zu erfüllen, oder bei dem Finanzunternehmen andere Formen nachteiliger Auswirkungen, einschließlich großer Verluste, herbeiführen oder die finanzielle Stabilität der Union insgesamt gefährden könnten;

30. „Leitungsorgan“ ein Leitungsorgan im Sinne von Artikel 4 Absatz 1 Nummer 36 der Richtlinie 2014/65/EU, von Artikel 3 Absatz 1 Nummer 7 der Richtlinie 2013/36/EU, von Artikel 2 Absatz 1 Buchstabe s der Richtlinie 2009/65/EG des Europäischen Parlaments und des Rates ([31]), von Artikel 2 Absatz 1 Nummer 45 der Verordnung (EU) Nr. 909/2014, von Artikel 3 Absatz 1 Nummer 20 der Verordnung (EU) 2016/1011 sowie im Sinne der einschlägigen Vorschrift der Verordnung über Märkte von Krypto-Werten oder die entsprechenden Personen, die das Unternehmen tatsächlich leiten oder im Einklang mit dem einschlägigen Unionsrecht oder nationalen Recht Schlüsselfunktionen wahrnehmen;

31. „Kreditinstitut“ ein Kreditinstitut im Sinne von Artikel 4 Absatz 1 Nummer 1 der Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates ([32]);

32. „nach der Richtlinie 2013/36/EU ausgenommenes Institut“ eine in Artikel 2 Absatz 5 Nummern 4 bis 23 der Richtlinie 2013/36/EU aufgeführte Einrichtung;

33. „Wertpapierfirma“ eine Wertpapierfirma im Sinne von Artikel 4 Absatz 1 Nummer 1 der Richtlinie 2014/65/EU;

34. „kleine und nicht verflochtene Wertpapierfirma“ eine Wertpapierfirma, die die in Artikel 12 Absatz 1 der Verordnung (EU) 2019/2033 des Europäischen Parlaments und des Rates ([33]) genannten Bedingungen erfüllt;

35. „Zahlungsinstitut“ ein Zahlungsinstitut im Sinne von Artikel 4 Nummer 4 der Richtlinie (EU) 2015/2366;

36. „nach der Richtlinie (EU) 2015/2366 ausgenommenes Zahlungsinstitut“ ein Zahlungsinstitut, für das eine Ausnahme nach Artikel 32 Absatz 1 der Richtlinie (EU) 2015/2366 gilt;

37. „Kontoinformationsdienstleister“ einen Kontoinformationsdienstleister im Sinne von Artikel 33 Absatz 1 der Richtlinie (EU) 2015/2366;

38. „E-Geld-Institut“ ein E-Geld-Institut im Sinne von Artikel 2 Nummer 1 der Richtlinie 2009/110/EG;

39. „nach der Richtlinie 2009/110/EG ausgenommenes E-Geld-Institut“ ein E-Geld-Institut, für das eine Ausnahme nach Artikel 9 Absatz 1 der Richtlinie 2009/110/EG gilt;

40. „zentrale Gegenpartei“ eine zentrale Gegenpartei im Sinne von Artikel 2 Nummer 1 der Verordnung (EU) Nr. 648/2012;

41. „Transaktionsregister“ ein Transaktionsregister im Sinne von Artikel 2 Nummer 2 der Verordnung (EU) Nr. 648/2012;

42. „Zentralverwahrer“ ein Zentralverwahrer im Sinne von Artikel 2 Absatz 1 Nummer 1 der Verordnung (EU) Nr. 909/2014;

43. „Handelsplatz“ einen Handelsplatz im Sinne von Artikel 4 Absatz 1 Nummer 24 der Richtlinie 2014/65/EU.

44. „Verwalter alternativer Investmentfonds“ einen Verwalter alternativer Investmentfonds im Sinne von Artikel 4 Absatz 1 Buchstabe b der Richtlinie 2011/61/EU;

45. „Verwaltungsgesellschaft“ eine Verwaltungsgesellschaft im Sinne von Artikel 2 Absatz 1 Buchstabe b der Richtlinie 2009/65/EG.

46. „Datenbereitstellungsdienst“ einen in Artikel 2 Absatz 1 Nummern 34 bis 36 der Verordnung (EU) Nr. 600/2014 genannten Datenbereitstellungsdienst im Sinne der genannten Verordnung;

47. „Versicherungsunternehmen“ ein Versicherungsunternehmen im Sinne von Artikel 13 Nummer 1 der Richtlinie 2009/138/EG;

48. „Rückversicherungsunternehmen“ ein Rückversicherungsunternehmen im Sinne von Artikel 13 Nummer 4 der Richtlinie 2009/138/EG;

([31]) Richtlinie 2009/65/EG des Europäischen Parlaments und des Rates vom 13. Juli 2009 zur Koordinierung der Rechts- und Verwaltungsvorschriften betreffend bestimmte Organismen für gemeinsame Anlagen in Wertpapieren (OGAW) (ABl. L 302 vom 17.11.2009, S. 32).

([32]) Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über Aufsichtsanforderungen an Kreditinstitute und zur Änderung der Verordnung (EU) Nr. 648/2012 (ABl. L 176 vom 27.6.2013, S. 1).

([33]) Verordnung (EU) 2019/2033 des Europäischen Parlaments und des Rates vom 27. November 2019 über Aufsichtsanforderungen an Wertpapierfirmen und zur Änderung der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 575/2013, (EU) Nr. 600/2014 und (EU) Nr. 806/2014 (ABl. L 314 vom 5.12.2019, S. 1).

49. „Versicherungsvermittler“ einen Versicherungsvermittler im Sinne von Artikel 2 Absatz 1 Nummer 3 der Richtlinie (EU) 2016/97 des Europäischen Parlaments und des Rates ([34]);

50. „Versicherungsvermittler in Nebentätigkeit“ einen Versicherungsvermittler in Nebentätigkeit im Sinne von Artikel 2 Absatz 1 Nummer 4 der Richtlinie (EU) 2016/97;

51. „Rückversicherungsvermittler“ einen Rückversicherungsvermittler im Sinne von Artikel 2 Absatz 1 Nummer 5 der Richtlinie (EU) 2016/97;

52. „Einrichtung der betrieblichen Altersversorgung“ eine Einrichtung der betrieblichen Altersversorgung im Sinne von Artikel 6 Nummer 1 der Richtlinie (EU) 2016/2341;

53. „kleine Einrichtung der betrieblichen Altersversorgung“ eine Einrichtung der betrieblichen Altersversorgung, die Altersversorgungssysteme mit insgesamt weniger als 100 Versorgungsanwärtern betreibt;

54. „Ratingagentur“ eine Ratingagentur im Sinne von Artikel 3 Absatz 1 Buchstabe b der Verordnung (EG) Nr. 1060/2009;

55. „Anbieter von Krypto-Dienstleistungen“ einen Anbieter von Krypto-Dienstleistungen im Sinne der einschlägigen Vorschrift der Verordnung über Märkte von Krypto-Werten;

56. „Emittent wertreferenzierter Token“ einen Emittenten „wertreferenzierter Token“ im Sinne der einschlägigen Vorschrift der Verordnung über Märkte von Krypto-Werten;

57. „Administrator kritischer Referenzwerte“ einen Administrator „kritischer Referenzwerte“ im Sinne von Artikel 3 Absatz 1 Nummer 25 der Verordnung (EU) 2016/1011;

58. „Schwarmfinanzierungsdienstleister“ einen Schwarmfinanzierungsdienstleister im Sinne von Artikel 2 Absatz 1 Buchstabe e der Verordnung (EU) 2020/1503 des Europäischen Parlaments und des Rates ([35]);

59. „Verbriefungsregister“ ein Verbriefungsregister im Sinne von Artikel 2 Nummer 23 der Verordnung (EU) 2017/2402 des Europäischen Parlaments und des Rates ([36]);

60. „Kleinstunternehmen“ ein Finanzunternehmen, bei dem es sich nicht um einen Handelsplatz, eine zentrale Gegenpartei, ein Transaktionsregister oder einen Zentralverwahrer handelt, das weniger als zehn Personen beschäftigt und dessen Jahresumsatz bzw. -bilanzsumme 2 Mio. EUR nicht überschreitet;

61. „federführende Überwachungsbehörde“ die gemäß Artikel 31 Absatz 1 Buchstabe b dieser Verordnung benannte Europäische Aufsichtsbehörde;

62. „Gemeinsamer Ausschuss“ den jeweils in Artikel 54 der Verordnung (EU) Nr. 1093/2010, der Verordnung (EU) Nr. 1094/2010 und der Verordnung (EU) Nr. 1095/2010 genannten Ausschuss;

63. „Kleinunternehmen“ ein Finanzunternehmen, das 10 oder mehr, aber weniger als 50 Personen beschäftigt und dessen Jahresumsatz bzw. -bilanzsumme 2 Mio. EUR überschreitet, nicht jedoch 10 Mio. EUR;

64. „mittleres Unternehmen“ ein Finanzunternehmen, das kein Kleinunternehmen ist, das weniger als 250 Personen beschäftigt und dessen Jahresumsatz 50 Mio. EUR und/oder dessen Jahresbilanzsumme 43 Mio. EUR nicht überschreitet;

65. „staatliche Behörde“ jede staatliche Stelle oder sonstige Stelle der öffentlichen Verwaltung, einschließlich der nationalen Zentralbanken.

([34]) Richtlinie (EU) 2016/97 des Europäischen Parlaments und des Rates vom 20. Januar 2016 über Versicherungsvertrieb (ABl. L 26 vom 2.2.2016, S. 19).

([35]) Verordnung (EU) 2020/1503 des Europäischen Parlaments und des Rates vom 7. Oktober 2020 über Europäische Schwarmfinanzierungsdienstleister für Unternehmen und zur Änderung der Verordnung (EU) 2017/1129 und der Richtlinie (EU) 2019/1937 (ABl. L 347 vom 20.10.2020, S. 1).

([36]) Verordnung (EU) 2017/2402 des Europäischen Parlaments und des Rates vom 12. Dezember 2017 zur Festlegung eines allgemeinen Rahmens für Verbriefungen und zur Schaffung eines spezifischen Rahmens für einfache, transparente und standardisierte Verbriefung und zur Änderung der Richtlinien 2009/65/EG, 2009/138/EG, 2011/61/EU und der Verordnungen (EG) Nr. 1060/2009 und (EU) Nr. 648/2012 (ABl. L 347 vom 28.12.2017, S. 35).

Artikel 4

Grundsatz der Verhältnismäßigkeit

(1) Die Finanzunternehmen wenden die in Kapitel II festgelegten Vorschriften im Einklang mit dem Grundsatz der Verhältnismäßigkeit an, wobei ihrer Größe und ihrem Gesamtrisikoprofil sowie der Art, dem Umfang und der Komplexität ihrer Dienstleistungen, Tätigkeiten und Geschäfte Rechnung zu tragen ist.

(2) Darüber hinaus muss die Anwendung der Kapitel III und IV sowie des Kapitels V Abschnitt I durch die Finanzunternehmen in einem angemessenen Verhältnis zu ihrer Größe und ihrem Gesamtrisikoprofil sowie zu der Art, dem Umfang und der Komplexität ihrer Dienstleistungen, Tätigkeiten und Geschäfte stehen, wie dies in den einschlägigen Vorschriften jener Kapitel ausdrücklich vorgesehen ist.

(3) Bei der Überprüfung der Kohärenz des IKT-Risikomanagementrahmens auf der Grundlage der Berichte, die den zuständigen Behörden gemäß Artikel 6 Absatz 5 und Artikel 16 Absatz 2 auf Anfrage vorgelegt werden, prüfen die zuständigen Behörden die Anwendung des Grundsatzes der Verhältnismäßigkeit durch die Finanzunternehmen.

KAPITEL II

IKT-Risikomanagement

Abschnitt I

Artikel 5

Governance und Organisation

(1) Finanzunternehmen verfügen über einen internen Governance- und Kontrollrahmen, der im Einklang mit Artikel 6 Absatz 4 ein wirksames und umsichtiges Management von IKT-Risiken gewährleistet, um ein hohes Niveau an digitaler operationaler Resilienz zu erreichen.

(2) Das Leitungsorgan des Finanzunternehmens definiert, genehmigt, überwacht und verantwortet die Umsetzung aller Vorkehrungen im Zusammenhang mit dem IKT-Risikomanagementrahmen nach Artikel 6 Absatz 1.

Für die Zwecke von Unterabsatz 1 gilt Folgendes:

a) Das Leitungsorgan trägt die letztendliche Verantwortung für das Management der IKT-Risiken des Finanzunternehmens;

b) das Leitungsorgan führt Leitlinien ein, die darauf abzielen, hohe Standards in Bezug auf die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten aufrechtzuerhalten;

c) das Leitungsorgan legt klare Aufgaben und Verantwortlichkeiten für alle IKT-bezogenen Funktionen sowie angemessene Governance-Regelungen fest, um eine wirksame und rechtzeitige Kommunikation, Zusammenarbeit und Koordinierung zwischen diesen Funktionen zu gewährleisten;

d) das Leitungsorgan trägt die Gesamtverantwortung für die Festlegung und Genehmigung der Strategie für die digitale operationale Resilienz gemäß Artikel 6 Absatz 8, einschließlich der Festlegung der angemessenen Toleranzschwelle für das IKT-Risiko des Finanzunternehmens gemäß Artikel 6 Absatz 8 Buchstabe b;

e) das Leitungsorgan genehmigt, überwacht und überprüft regelmäßig die Umsetzung der in Artikel 11 Absatz 1 genannten IKT-Geschäftsfortführungsleitlinie und der in Artikel 11 Absatz 3 genannten IKT-Reaktions- und Wiederherstellungspläne, die als eigenständige spezielle Leitlinie, die integraler Bestandteil der allgemeinen Geschäftsfortführungsleitlinie des Finanzunternehmens und seines Reaktions- und Wiederherstellungsplans ist, verabschiedet werden können;

f) das Leitungsorgan genehmigt und überprüft regelmäßig die internen IKT-Revisionspläne des Finanzunternehmens, die IKT-Revision und die daran vorgenommenen wesentlichen Änderungen;

g) das Leitungsorgan weist angemessene Budgetmittel zu und überprüft diese regelmäßig, um den Anforderungen des Finanzunternehmens an die digitale operationale Resilienz in Bezug auf alle Arten von Ressourcen gerecht zu werden, einschließlich einschlägiger Programme zur Sensibilisierung für IKT-Sicherheit und Schulungen zur digitalen operationalen Resilienz nach Artikel 13 Absatz 6 sowie IKT-Kompetenzen für alle Mitarbeiter;

h) das Leitungsorgan genehmigt und überprüft regelmäßig die Leitlinie des Finanzunternehmens in Bezug auf Vereinbarungen über die Nutzung von IKT-Dienstleistungen, die von IKT-Drittdienstleistern bereitgestellt werden;

i) das Leitungsorgan richtet auf Unternehmensebene Meldekanäle ein, die es ihm ermöglichen, ordnungsgemäß über Folgendes informiert zu werden:

   i) mit IKT-Drittdienstleistern geschlossene Vereinbarungen über die Nutzung von IKT-Dienstleistungen,

   ii) alle relevanten geplanten wesentlichen Änderungen in Bezug auf die IKT-Drittdienstleister,

   iii) die potenziellen Auswirkungen derartiger Änderungen auf die kritischen oder wichtigen Funktionen, die Gegenstand dieser Vereinbarungen sind, einschließlich einer Zusammenfassung der Risikoanalyse, um die Auswirkungen dieser Änderungen zu bewerten, und zumindest über schwerwiegende IKT-bezogene Vorfälle und deren Auswirkungen sowie über Gegen-, Wiederherstellungs- und Korrekturmaßnahmen.

(3) Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, richten eine Funktion ein, um die mit IKT-Drittdienstleistern über die Nutzung von IKT-Dienstleistungen geschlossenen Vereinbarungen zu überwachen, oder benennen ein Mitglied der Geschäftsleitung, das für die Überwachung der damit verbundenen Risikoexposition und die einschlägige Dokumentation verantwortlich ist.

(4) Die Mitglieder des Leitungsorgans des Finanzunternehmens halten ausreichende Kenntnisse und Fähigkeiten aktiv auf dem neuesten Stand — unter anderem indem sie regelmäßig spezielle Schulungen absolvieren — entsprechend den zu managenden IKT-Risiken, um die IKT-Risiken und deren Auswirkungen auf die Geschäftstätigkeit des Finanzunternehmens verstehen und bewerten können.

Abschnitt II

Artikel 6

IKT-Risikomanagementrahmen

(1) Finanzunternehmen verfügen über einen soliden, umfassenden und gut dokumentierten IKT-Risikomanagementrahmen, der Teil ihres Gesamtrisikomanagementsystems ist und es ihnen ermöglicht, IKT-Risiken schnell, effizient und umfassend anzugehen und ein hohes Niveau an digitaler operationaler Resilienz zu gewährleisten.

(2) Der IKT-Risikomanagementrahmen umfasst mindestens Strategien, Leit- und Richtlinien, Verfahren sowie IKT-Protokolle und -Tools, die erforderlich sind, um alle Informations- und IKT-Assets, einschließlich Computer-Software, Hardware und Server, ordnungsgemäß und angemessen zu schützen sowie um alle relevanten physischen Komponenten und Infrastrukturen, wie etwa Räumlichkeiten, Rechenzentren und ausgewiesene sensible Bereiche zu schützen, damit der angemessene Schutz aller Informations- und IKT-Assets vor Risiken, einschließlich der Beschädigung und des unbefugten Zugriffs oder der unbefugten Nutzung, gewährleistet ist.

(3) Im Einklang mit ihrem IKT-Risikomanagementrahmen minimieren Finanzunternehmen die Auswirkungen von IKT-Risiken, indem sie geeignete Strategien, Leit- und Richtlinien, Verfahren, IKT-Protokolle und Tools einsetzen. Sie legen den zuständigen Behörden auf Anfrage vollständige und aktuelle Informationen über IKT-Risiken und ihren IKT-Risikomanagementrahmen vor.

(4) Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, übertragen die Zuständigkeit für das Management und die Überwachung des IKT-Risikos an eine Kontrollfunktion und stellen ein angemessenes Maß an Unabhängigkeit dieser Kontrollfunktion sicher, um Interessenkonflikte zu vermeiden. Die Finanzunternehmen sorgen für eine angemessene Trennung und Unabhängigkeit von IKT-Risikomanagementfunktionen, Kontrollfunktionen und internen Revisionsfunktionen gemäß dem Modell der drei Verteidigungslinien oder einem internen Modell für Risikomanagement und Kontrolle.

(5) Der IKT-Risikomanagementrahmen wird mindestens einmal jährlich — bzw. im Falle von Kleinstunternehmen regelmäßig — sowie bei Auftreten schwerwiegender IKT-bezogener Vorfälle und nach aufsichtsrechtlichen Anweisungen oder Feststellungen, die sich aus einschlägigen Tests der digitalen operationalen Resilienz oder Auditverfahren ergeben, dokumentiert und überprüft. Der Rahmen wird auf Grundlage der bei Umsetzung und Überwachung gewonnenen Erkenntnisse kontinuierlich verbessert. Der zuständigen Behörde wird auf deren Anfrage ein Bericht über die Überprüfung des IKT-Risikomanagementrahmens vorgelegt.

(6) Im Einklang mit dem Revisionsplan des betreffenden Finanzunternehmens ist der IKT-Risikomanagementrahmen von Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, regelmäßig einer internen Revision durch Revisoren zu unterziehen. Diese Revisoren verfügen über ausreichendes Wissen und ausreichende Fähigkeiten und Fachkenntnisse im Bereich IKT-Risiken sowie über eine angemessene Unabhängigkeit. Häufigkeit und Schwerpunkt von IKT-Revisionen sind den IKT-Risiken des Finanzunternehmens entsprechend angemessen.

(7) Auf der Grundlage der Feststellungen aus der Überprüfung der internen Revision legen Finanzunternehmen ein förmliches Follow-up-Verfahren einschließlich Regeln für die rechtzeitige Überprüfung und Auswertung kritischer Erkenntnisse der IKT-Revision fest.

(8) Der IKT-Risikomanagementrahmen umfasst eine Strategie für die digitale operationale Resilienz, in der dargelegt wird, wie der Rahmen umgesetzt wird. Zu diesem Zweck schließt die Strategie für die digitale operationale Resilienz Methoden, um IKT-Risiken anzugehen und spezifische IKT-Ziele zu erreichen, ein, indem

a) erläutert wird, wie der IKT-Risikomanagementrahmen die Geschäftsstrategie und die Ziele des Finanzunternehmens unterstützt;

b) die Risikotoleranzschwelle für IKT-Risiken im Einklang mit der Risikobereitschaft des Finanzunternehmens festgelegt und die Auswirkungsstoleranz mit Blick auf IKT-Störungen untersucht wird;

c) klare Ziele für die Informationssicherheit festgelegt werden, einschließlich der wesentlichen Leistungsindikatoren und der wesentlichen Risikokennzahlen;

d) die IKT-Referenzarchitektur und etwaige Änderungen erläutert werden, die für die Erreichung spezifischer Geschäftsziele erforderlich sind;

e) die verschiedenen Mechanismen dargelegt werden, die eingesetzt wurden, um IKT-bezogene Vorfälle zu erkennen, sich davor zu schützen und daraus entstehende Folgen zu verhindern;

f) der aktuelle Stand bezüglich der digitalen operationalen Resilienz anhand der Anzahl gemeldeter schwerwiegender IKT-Vorfälle und bezüglich der Wirksamkeit von Präventivmaßnahmen dargelegt wird;

g) Tests der digitalen operationalen Resilienz gemäß Kapitel IV dieser Verordnung durchgeführt werden;

h) für IKT-bezogene Vorfälle eine Kommunikationsstrategie dargelegt wird, die gemäß Artikel 14 offengelegt werden muss.

(9) Finanzunternehmen können im Zusammenhang mit der Strategie für die digitale operationale Resilienz nach Absatz 8 eine ganzheitliche Strategie zur Nutzung mehrerer IKT-Anbieter auf Gruppen- oder Unternehmensebene festlegen, in der wesentliche Abhängigkeiten von IKT-Drittdienstleistern aufgezeigt und die Gründe für die Nutzung verschiedener IKT-Drittdienstleister erläutert werden.

(10) Finanzunternehmen können die Überprüfung der Einhaltung der Anforderungen für das IKT-Risikomanagement im Einklang mit den sektorspezifischen Rechtsvorschriften der Union und der Mitgliedstaaten an gruppeninterne oder externe Unternehmen auslagern. Im Falle einer solchen Auslagerung bleibt das Finanzunternehmen weiterhin uneingeschränkt für die Überprüfung der Einhaltung der IKT-Risikomanagementanforderungen verantwortlich.

Artikel 7

IKT-Systeme, -Protokolle und -Tools

Um IKT-Risiken zu bewältigen und zu managen, verwenden und unterhalten Finanzunternehmen stets auf dem neuesten Stand zu haltende IKT-Systeme, -Protokolle und -Tools, die

a) dem Umfang von Vorgängen, die die Ausübung ihrer Geschäftstätigkeiten unterstützen, im Einklang mit dem Grundsatz der Verhältnismäßigkeit nach Artikel 4 angemessen sind;

b) zuverlässig sind;

c) mit ausreichenden Kapazitäten ausgestattet sind, um die Daten, die für die Ausführung von Tätigkeiten und die rechtzeitige Erbringung von Dienstleistungen erforderlich sind, genau zu verarbeiten und Auftragsspitzen, Mitteilungen oder Transaktionen auch bei Einführung neuer Technologien bewältigen zu können;

d) technologisch resilient sind, um dem unter angespannten Marktbedingungen oder anderen widrigen Umständen erforderlichen zusätzlichen Bedarf an Informationsverarbeitung angemessen zu begegnen.

Artikel 8

Identifizierung

(1) Als Teil des IKT-Risikomanagementrahmens gemäß Artikel 6 Absatz 1 ermitteln und klassifizieren Finanzunternehmen alle IKT-gestützten Unternehmensfunktionen, Rollen und Verantwortlichkeiten, die Informations- und IKT-Assets, die diese Funktionen unterstützen, sowie deren Rollen und Abhängigkeiten hinsichtlich der IKT-Risiken und dokumentieren sie angemessen. Finanzunternehmen überprüfen erforderlichenfalls, mindestens jedoch einmal jährlich, ob diese Klassifizierung und jegliche einschlägige Dokumentation angemessen sind.

(2) Finanzunternehmen ermitteln kontinuierlich alle Quellen für IKT-Risiken, insbesondere das Risiko gegenüber und von anderen Finanzunternehmen, und bewerten Cyberbedrohungen und IKT-Schwachstellen, die für ihre IKT-gestützten Geschäftsfunktionen, Informations- und IKT-Assets relevant sind. Finanzunternehmen überprüfen regelmäßig, mindestens jedoch einmal jährlich die sie betreffenden Risikoszenarien.

(3) Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, führen bei jeder wesentlichen Änderung der Netzwerk- und Informationssysteminfrastruktur, der Prozesse oder Verfahren, die sich auf ihre IKT-gestützten Unternehmensfunktionen, Informations- oder IKT-Assets auswirken, eine Risikobewertung durch.

(4) Finanzunternehmen ermitteln alle Informations- und IKT-Assets, einschließlich derer an externen Standorten, Netzwerkressourcen und Hardware, und erfassen diejenigen, die als kritisch gelten. Sie erfassen die Konfiguration von Informations- und IKT-Assets sowie die Verbindungen und Interdependenzen zwischen den verschiedenen Informations- und IKT-Assets.

(5) Finanzunternehmen ermitteln und dokumentieren alle Prozesse, die von IKT-Drittdienstleistern abhängen, und ermitteln Vernetzungen mit IKT-Drittdienstleistern, die Dienste zur Unterstützung kritischer oder wichtiger Funktionen bereitstellen.

(6) Für die Zwecke der Absätze 1, 4 und 5 führen Finanzunternehmen entsprechende Inventare, die sie regelmäßig sowie bei jeder wesentlichen Änderung im Sinne von Absatz 3 aktualisieren.

(7) Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, führen für alle IKT-Altsysteme regelmäßig, mindestens jedoch einmal jährlich und in jedem Fall vor und nach Anschluss von Technologien, Anwendungen oder Systemen eine spezifische Bewertung des IKT-Risikos durch.

Artikel 9

Schutz und Prävention

(1) Um einen angemessenen Schutz von IKT-Systemen zu gewährleisten und Gegenmaßnahmen zu organisieren, überwachen und kontrollieren Finanzunternehmen kontinuierlich die Sicherheit und das Funktionieren der IKT-Systeme und -Tools und minimieren durch den Einsatz angemessener IKT-Sicherheitstools, -Richtlinien und -Verfahren die Auswirkungen von IKT-Risiken auf IKT-Systeme.

(2) Finanzunternehmen konzipieren, beschaffen und implementieren IKT-Sicherheitsrichtlinien, -verfahren, -protokolle und -Tools, die darauf abzielen, die Resilienz, Kontinuität und Verfügbarkeit von IKT-Systemen, insbesondere jener zur Unterstützung kritischer oder wichtiger Funktionen, zu gewährleisten und hohe Standards in Bezug auf die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit, von Daten aufrechtzuerhalten, unabhängig davon, ob diese Daten gespeichert sind oder gerade verwendet oder übermittelt werden.

(3) Um die in Absatz 2 genannten Ziele zu erreichen, greifen Finanzunternehmen auf IKT-Lösungen und -Prozesse zurück, die gemäß Artikel 4 angemessen sind. Diese IKT-Lösungen und -Prozesse müssen

a) die Sicherheit der Datenübermittlungsmittel gewährleisten;

b) das Risiko von Datenkorruption oder -verlust, unbefugtem Zugriff und technischen Mängeln, die die Geschäftstätigkeit beeinträchtigen können, minimieren;

c) dem Mangel an Verfügbarkeit, der Beeinträchtigung der Authentizität und Integrität, den Verletzungen der Vertraulichkeit und dem Verlust von Daten vorbeugen;

d) gewährleisten, dass Daten vor Risiken, die beim Datenmanagement entstehen, einschließlich schlechter Verwaltung, verarbeitungsbedingter Risiken und menschlichem Versagen, geschützt werden.

(4) Als Teil des IKT-Risikomanagementrahmens nach Artikel 6 Absatz 1 gilt für Finanzunternehmen Folgendes:

a) Sie erarbeiten und dokumentieren eine Informationssicherheitsleitlinie, in der Regeln zum Schutz der Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten und der Informations- und IKT-Assets, gegebenenfalls einschließlich derjenigen ihrer Kunden, festgelegt sind;

b) sie richten entsprechend einem risikobasierten Ansatz eine solide Struktur für Netzwerk- und Infrastrukturmanagement unter Verwendung angemessener Techniken, Methoden und Protokolle ein, wozu auch die Umsetzung automatisierter Mechanismen zur Isolierung betroffener Informationsassets im Falle von Cyberangriffen gehören kann;

c) sie implementieren Richtlinien, die den physischen oder logischen Zugang zu Informations- und IKT-Assets ausschließlich auf den Umfang beschränken, der für rechtmäßige und zulässige Funktionen und Tätigkeiten erforderlich ist, und legen zu diesem Zweck eine Reihe von Konzepten, Verfahren und Kontrollen fest, die auf Zugangs- und Zugriffsrechte gerichtet sind, und gewährleisten deren gründliche Verwaltung;

d) sie implementieren Konzepte und Protokolle für starke Authentifizierungsmechanismen, die auf einschlägigen Normen und speziellen Kontrollsystemen basieren, sowie Schutzmaßnahmen für kryptografische Schlüssel, wobei Daten auf der Grundlage der Ergebnisse aus genehmigten Datenklassifizierungs- und IKT-Risikobewertungsprozessen verschlüsselt werden;

e) sie implementieren und dokumentieren Richtlinien, Verfahren und Kontrollen für das IKT-Änderungsmanagement, einschließlich Änderungen an Software, Hardware, Firmware-Komponenten, den Systemen oder von Sicherheitsparametern, die auf einem Risikobewertungsansatz basieren und fester Bestandteil des gesamten Änderungsmanagementprozesses des Finanzunternehmens sind, um sicherzustellen, dass alle Änderungen an IKT-Systemen auf kontrollierte Weise erfasst, getestet, bewertet, genehmigt, implementiert und überprüft werden;

f) sie besitzen angemessene und umfassende dokumentierte Richtlinien für Patches und Updates.

Für die Zwecke von Unterabsatz 1 Buchstabe b konzipieren Finanzunternehmen die Infrastruktur für die Netzanbindung und Netzwerkverbindung so, dass sie sofort getrennt oder segmentiert werden kann, damit eine Ansteckung, insbesondere bei miteinander verbundenen Finanzprozessen, minimiert und verhindert wird.

Für die Zwecke von Unterabsatz 1 Buchstabe e wird das Verfahren für das IKT-Änderungsmanagement von zuständigen Leitungsebenen genehmigt und hat spezifische Protokolle.

Artikel 10

Erkennung

(1) Finanzunternehmen verfügen über Mechanismen, um anomale Aktivitäten im Einklang mit Artikel 17, darunter auch Probleme bei der Leistung von IKT-Netzwerken und IKT-bezogene Vorfälle, umgehend zu erkennen und potenzielle einzelne wesentliche Schwachstellen zu ermitteln.

Alle in Unterabsatz 1 aufgeführten Erkennungsmechanismen werden gemäß Artikel 25 regelmäßig getestet.

(2) Die in Absatz 1 genannten Erkennungsmechanismen ermöglichen mehrere Kontrollebenen und legen Alarmschwellen und -kriterien fest, um Reaktionsprozesse bei IKT-bezogenen Vorfällen auszulösen und einzuleiten, einschließlich automatischer Warnmechanismen für Mitarbeiter, die für Reaktionsmaßnahmen bei IKT-bezogenen Vorfällen zuständig sind.

(3) Finanzunternehmen stellen ausreichende Ressourcen und Kapazitäten bereit, um Nutzeraktivitäten, das Auftreten von IKT-Anomalien und IKT-bezogenen Vorfällen, darunter insbesondere Cyberangriffe, zu überwachen.

(4) Datenbereitstellungsdienste verfügen darüber hinaus über Systeme, mit denen wirksam Handelsauskünfte auf Vollständigkeit geprüft, Lücken und offensichtliche Fehler erkannt und eine Neuübermittlung angefordert werden können.

Artikel 11

Reaktion und Wiederherstellung

(1) Als Teil des in Artikel 6 Absatz 1 genannten IKT-Risikomanagementrahmens und auf der Grundlage der Identifizierungsanforderungen nach Artikel 8 legen Finanzunternehmen eine umfassende IKT-Geschäftsfortführungsleitlinie fest, die als eigenständige spezielle Leitlinie, die fester Bestandteil der allgemeinen Geschäftsfortführungsleitlinie des Finanzunternehmens ist, verabschiedet werden kann.

(2) Finanzunternehmen implementieren die IKT-Geschäftsfortführungsleitlinie mittels spezieller, angemessener und dokumentierter Regelungen, Pläne, Verfahren und Mechanismen, die darauf abzielen,

a) die Fortführung der kritischen oder wichtigen Funktionen des Finanzunternehmens sicherzustellen;

b) auf alle IKT-bezogenen Vorfälle rasch, angemessen und wirksam zu reagieren und diesen so entgegenzuwirken, dass Schäden begrenzt werden und die Wiederaufnahme von Tätigkeiten und Wiederherstellungsmaßnahmen Vorrang erhalten;

c) unverzüglich spezielle Pläne zu aktivieren, die Eindämmungsmaßnahmen, Prozesse und Technologien für alle Arten IKT-bezogener Vorfälle ermöglichen und weitere Schäden vermeiden, sowie maßgeschneiderte Verfahren zur Reaktion und Wiederherstellung gemäß Artikel 12 zu aktivieren;

d) vorläufige Auswirkungen, Schäden und Verluste einzuschätzen;

e) Kommunikations- und Krisenmanagementmaßnahmen festzulegen, die gewährleisten, dass allen relevanten internen Mitarbeitern und externen Interessenträgern im Sinne von Artikel 14 aktualisierte Informationen übermittelt werden, und die Meldung an die zuständigen Behörden gemäß Artikel 19 sicherstellen.

(3) Finanzunternehmen implementieren als Teil des in Artikel 6 Absatz 1 genannten IKT-Risikomanagementrahmens damit verbundene IKT-Reaktions- und Wiederherstellungspläne, die einer unabhängigen internen Revision zu unterziehen sind, sofern es sich bei dem Finanzunternehmen nicht um ein Kleinstunternehmen handelt.

(4) Finanzunternehmen erstellen, pflegen und testen regelmäßig angemessene IKT-Geschäftsfortführungspläne, insbesondere in Bezug auf kritische oder wichtige Funktionen, die ausgelagert oder durch vertragliche Vereinbarungen an IKT-Drittdienstleister vergeben werden.

(5) Als Teil der allgemeinen Geschäftsfortführungsleitlinie führen Finanzunternehmen eine Business-Impact-Analyse (BIA) der bestehenden Risiken für schwerwiegende Betriebsstörungen durch. Im Rahmen der BIA bewerten Finanzunternehmen die potenziellen Auswirkungen schwerwiegender Betriebsstörungen anhand quantitativer und qualitativer Kriterien, wobei sie gegebenenfalls interne und externe Daten und Szenarioanalysen heranziehen. Dabei werden die Kritikalität der identifizierten und erfassten Unternehmensfunktionen, Unterstützungsprozesse, Abhängigkeiten von Dritten und Informationsassets sowie deren Interdependenzen berücksichtigt. Die Finanzunternehmen stellen sicher, dass IKT-Assets und -Dienste in voller Übereinstimmung mit der BIA konzipiert und genutzt werden, insbesondere wenn es darum geht, die Redundanz aller kritischen Komponenten in angemessener Weise zu gewährleisten.

(6) Im Rahmen ihres umfassenden IKT-Risikomanagements gilt für Finanzunternehmen Folgendes:

a) sie testen bei IKT-Systemen, die alle Funktionen unterstützen, mindestens jährlich sowie im Falle jeglicher wesentlicher Änderungen an IKT-Systemen, die kritische oder wichtige Funktionen unterstützen, die IKT-Geschäftsfortführungspläne sowie die IKT-Reaktions- und Wiederherstellungspläne;

b) sie testen die gemäß Artikel 14 erstellten Krisenkommunikationspläne.

Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, nehmen für die Zwecke von Unterabsatz 1 Buchstabe a Szenarien für Cyberangriffe und Umstellungen von der primären IKT-Infrastruktur auf die redundanten Kapazitäten, Backups und Systeme, die für die Erfüllung der Verpflichtungen nach Artikel 12 erforderlich sind, in ihre Testpläne auf.

Finanzunternehmen überprüfen ihre IKT-Geschäftsfortführungsleitlinie und ihre IKT-Reaktions- und Wiederherstellungspläne regelmäßig und berücksichtigen dabei die Ergebnisse von Tests, die gemäß Unterabsatz 1 durchgeführt wurden, sowie die Empfehlungen, die sich aus Audits oder aufsichtlichen Überprüfungen ergeben.

(7) Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, verfügen über eine Krisenmanagementfunktion, die bei Aktivierung ihrer IKT- Geschäftsfortführungspläne oder ihrer IKT-Reaktions- und Wiederherstellungspläne unter anderem klare Verfahren für die Abwicklung interner und externer Krisenkommunikation gemäß Artikel 14 festlegt.

(8) Finanzunternehmen sorgen dafür, dass Aufzeichnungen über die Tätigkeiten vor und während Störungen, wenn ihre IKT-Geschäftsfortführungspläne oder ihre IKT-Reaktions- und Wiederherstellungspläne aktiviert werden, jederzeit eingesehen werden können.

(9) Zentralverwahrer übermitteln den zuständigen Behörden Kopien der Ergebnisse der Tests der IKT-Geschäftsfortführung oder ähnlicher Vorgänge.

(10) Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, melden den zuständigen Behörden auf Anfrage die geschätzten aggregierten jährlichen Kosten und Verluste, die durch schwerwiegende IKT-bezogene Vorfälle verursacht wurden.

(11) Gemäß jeweils Artikel 16 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 arbeiten die Europäischen Aufsichtsbehörden (im Folgenden „ESA“) über den Gemeinsamen Ausschuss bis zum 17. Juli 2024 gemeinsame Leitlinien für die Schätzung der aggregierten jährlichen Kosten und Verluste nach Absatz 10 aus.

Artikel 12

Richtlinie und Verfahren zum Backup sowie Verfahren und Methoden zur Wiedergewinnung und Wiederherstellung

(1) Um die Wiederherstellung von IKT-Systemen und Daten mit minimaler Ausfallzeit sowie begrenzten Störungen und Verlusten als Teil ihres IKT-Risikomanagementrahmens sicherzustellen, entwickeln und dokumentieren Finanzunternehmen:

a) Richtlinien und Verfahren für die Datensicherung, in denen der Umfang der Daten, die der Sicherung unterliegen, und die Mindesthäufigkeit der Sicherung auf der Grundlage der Kritikalität der Informationen oder des Vertraulichkeitsgrads der Daten festgelegt werden;

b) Wiedergewinnungs- und Wiederherstellungsverfahren und -methoden.

(2) Finanzunternehmen richten Datensicherungssysteme ein, die in Übereinstimmung mit den Richtlinien und Verfahren zur Datensicherung sowie den Verfahren und Methoden zur Wiedergewinnung und Wiederherstellung aktiviert werden können. Die Aktivierung von Datensicherungssystemen darf die Sicherheit der Netzwerk- und Informationssysteme oder die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten nicht gefährden. Die Datensicherungsverfahren sowie die Wiedergewinnungs- und Wiederherstellungsverfahren und -methoden sind regelmäßig zu testen.

(3) Bei der Wiedergewinnung gesicherter Daten mithilfe eigener Systeme verwenden Finanzunternehmen IKT-Systeme, die von ihrem Quellsystem physisch und logisch getrennt sind. Die IKT-Systeme müssen sicher vor unbefugtem Zugriff oder IKT-Manipulationen geschützt sein und die rechtzeitige Wiederherstellung von Diensten ermöglichen, wobei erforderlichenfalls Daten- und Systemsicherungen (Backups) zu nutzen sind.

Bei zentralen Gegenparteien ermöglichen die Wiederherstellungspläne die Wiederherstellung aller zum Zeitpunkt der Störung laufenden Transaktionen, damit die zentrale Gegenpartei weiterhin sicher arbeiten und die Abwicklung zum vorgesehenen Zeitpunkt abschließen kann.

Datenbereitstellungsdienste unterhalten zusätzlich angemessene Ressourcen und verfügen über die entsprechenden Sicherungs- und Wiedergewinnungseinrichtungen, damit ihre Dienste jederzeit angeboten und aufrechterhalten werden können.

(4) Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, unterhalten redundante IKT-Kapazitäten mit Ressourcen, Fähigkeiten und Funktionen, die für die Deckung des Geschäftsbedarfs ausreichen und angemessen sind. Kleinstunternehmen bewerten auf der Grundlage ihres Risikoprofils, ob diese redundanten IKT-Kapazitäten unterhalten werden müssen.

(5) Zentralverwahrer unterhalten mindestens einen sekundären Verarbeitungsstandort, dessen Ressourcen, Kapazitäten, Funktionen und Personalressourcen angemessen sind, um den Geschäftsbedarf zu decken.